DEPARTMENT OF THE NAVY

INFORMATION MANAGEMENT & INFORMATION TECHNOLOGY

Mid-Cycle Update
September 2008
Updates Highlighted

STRATEGIC PLAN

FY 2008 - 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 SEP 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of the Navy Information Management & Information Technology Strategic Plan	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Navy,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

FOREWORD

To meet the demands of the defense strategy, the Navy and Marine Corps must continue to operate effectively as a forward-postured, immediately employable force in Joint and multinational environments. The Service visions, Sea Power 21 and Marine Corps Strategy 21, recognize the challenges posed by a changing security environment and point the way to the future. The Navy and Marine Corps will leverage and integrate their respective strengths to produce a more effective and efficient Naval force with improved warfighting capabilities for the Joint force. The Naval Services will organize, deploy, employ, and sustain forces to conduct operations guided by the interrelated and complementary concepts of Sea Strike, Sea Shield, and Sea Basing integrated with the family of Marine Corps concepts, Expeditionary Maneuver Warfare, Operational Maneuver from the Sea, and Ship-to-Objective Maneuver; all of which will be enabled by FORCEnet.

Via FORCEnet, Expeditionary Naval Forces will integrate warriors, sensors, C2, platforms, and weapons into a networked, distributed, and sustainable combat force. FORCEnet will enhance situational awareness and decentralized decision making while compressing decision cycles and facilitating real-time collaborative planning, offensive and defensive power projection, and maneuver in time and space. Directly integrated with Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (JC4ISR), it will permit a dispersed Naval force to distribute or concentrate combat power as needed in an enlarged battlespace.

Use of FORCEnet will increase the effectiveness of Sea Strike, Sea Shield, Sea Basing, Expeditionary Maneuver Warfare, Operational Maneuver from the Sea, and Ship-to-Objective Maneuver, and thereby will facilitate integrated Naval forces and operations that are fully interoperable with other Joint forces. It will focus on creating information networks with new levels of connectivity and integration, which will provide common and consistent data throughout the force and integrate the force into the Joint information network. Netted sensors, processing, databases, applications, weapons, and forces will support dynamic C2 between Naval forces globally. Naval forces will leverage the connectivity provided by FORCEnet systems to expand operational reach, permitting offensive and defensive power projection of weapons and maneuver forces over vast areas from a dispersed sea base. Initial efforts will create a web-enabled environment transitioning stove-piped, legacy systems into an interoperable system of systems. The network will link new capabilities with legacy systems and reachback to databases, providing greater access to information. Redundant and incompatible legacy systems will be phased out. Network defensive measures will incorporate defense in breadth to ensure that networks are reliable.

This Naval Operating Concept for Joint Operations emphasizes the benefits that integrated Naval operations bring to Joint warfighting. As the Navy and Marine Corps integrate their warfighting capabilities, we are committed to achieving maximum interoperability and complementarity with the Army, Air Force, Coast Guard, and Special Operations Command in future Joint operations.

From Naval Operating Concept for Joint Operations, 2006

SECRETARY OF THE NAVY
The Honorable
Donald C. Winter

COMMANDANT OF THE MARINE CORPS
General James T. Conway

CHIEF OF NAVAL OPERATIONS
Admiral Gary Roughead

FROM THE DON IM AND IT LEADERSHIP TEAM

> *"Our goal is to connect our IM/IT initiatives to the men and women at the tip of the spear, whether they are aboard a destroyer or deployed to a forward operating base in Iraq. Accordingly, we must bring speed and a sense of urgency to all that we do."*
>
> Robert J. Carey
> Department of the Navy Chief Information Officer
> September 2007

Information Management (IM) and Information Technology (IT) in the Department of the Navy (DON) provide Navy and Marine Corps warfighters with the tools required to win. What we do begins and ends with the warfighter. Information Management is a value chain that ends in knowledge, providing the warfighter the ability to make informed decisions. This strategic plan describes the Department's vision, mission, governing principles, goals, objectives, and key performance indicators for IM/IT to support the warfighter. It is driven by, and aligned to, the overarching departmental goals articulated by the Secretary of the Navy.

To accomplish our mission, we must provide the foundation for success by providing the right IM/IT tools and infrastructure for the warfighter. We are in the process of right-sizing our architecture by moving away from the practice of buying new servers and networks for each new application and instead, building a common computing infrastructure. Similarly, we are also moving away from vendor-centric applications to a Service Oriented Architecture so the warfighters and those who support them can more easily access the tools and data they need, regardless of location or operating platform. At the same time, we must enhance our security capabilities while balancing the users' need for access.

As a Department, we must be smarter about leveraging our limited resources through effective IM/IT governance. To this end, we should manage our application portfolio, requiring a clear strategic or financial return for each IM/IT investment to ensure the warfighter is getting the best return on investment. This includes moving from decentralized to centralized management where it makes sense. The Command Information Officer serves an important role as the principal advisor to his or her Commander for issues regarding IM and alignment of IT investments to business priorities and assigned missions. Our decision making should be architecture driven, balancing people, process, and technology as a basic function of how we do business.

The intent of this plan is to assist DON leadership by providing a vision that describes desired departmental outcomes and identifies how they will be achieved and measured. For our commands, this plan will help strengthen their alignment to DON IM/IT goals and help clarify resource priorities. For the IM/IT workforce, this plan provides understanding of the direction of IM/IT in the DON, and how their contributions support this broader vision.

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
Robert J. Carey

DEPARTMENT OF THE NAVY
DEPUTY CIO
John J. Lussier

DEPARTMENT OF THE NAVY
DEPUTY CIO (NAVY)
VADM Harry B. Harris

DEPARTMENT OF THE NAVY
DEPUTY CIO (MARINE CORPS)
BGen George J. Allen

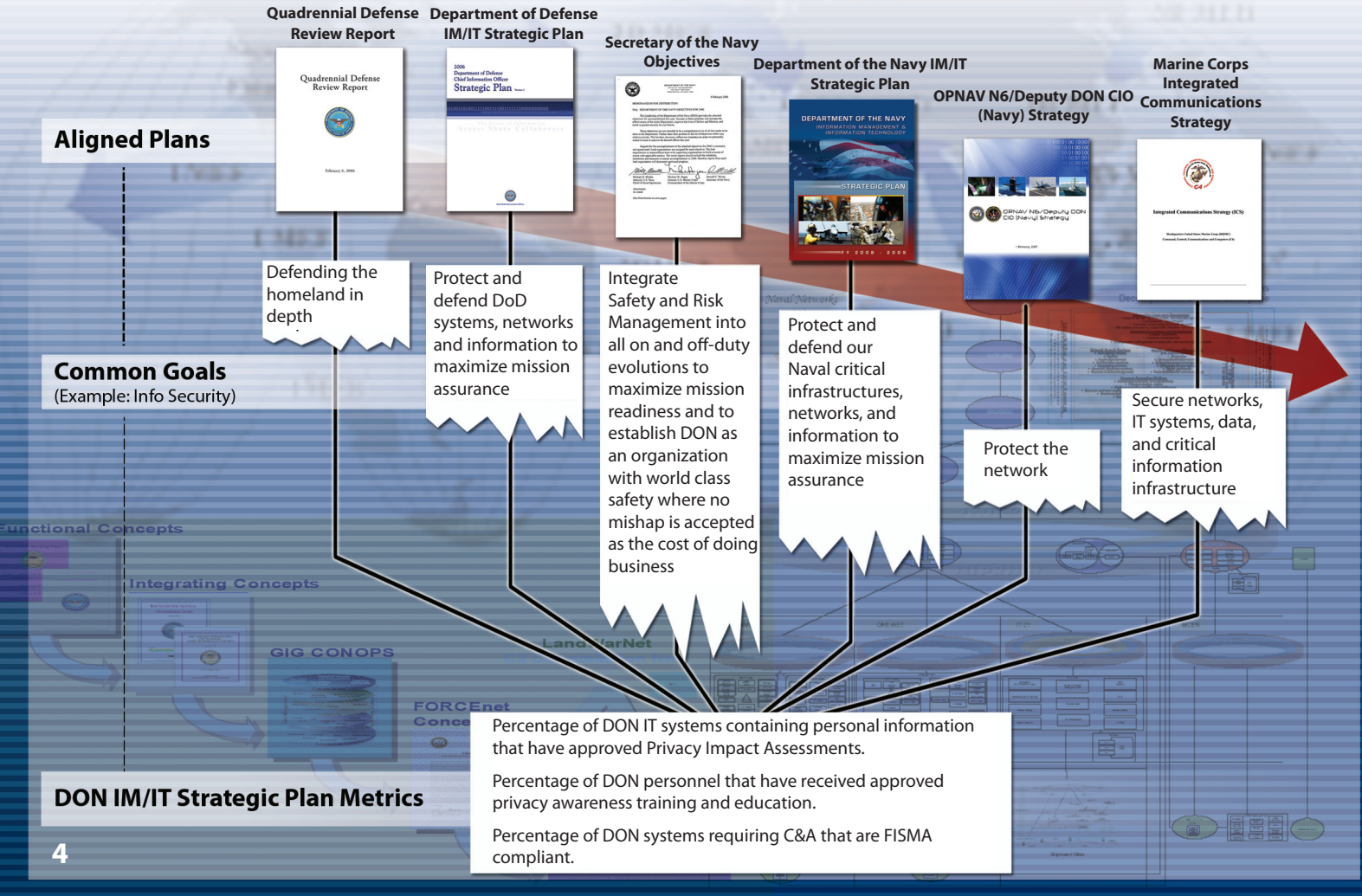
DEPARTMENT OF THE NAVY IM/IT STRATEGIC ALIGNMENT

> *"Developing and maintaining capable Naval forces requires our Nation to take a long-term view. It requires time, constant strategic planning, and significant commitment of resources to develop and maintain the world's premiere Naval force."*
>
> The Honorable Donald C. Winter
> Secretary of the Navy
> March 2007

Wars of the 21st century, including the Global War on Terrorism (GWOT), are increasingly being fought using net-centric warfighting techniques requiring close integration at multiple technology levels – networking, data, applications, and infrastructure. To continue delivering and expanding our net-centric capabilities, the *DON IM/IT Strategic Plan* is aligned to and driven by the warfighting requirements outlined in the *Quadrennial Defense Review Report*, the *Department of Defense CIO Strategic Plan*, and the *Secretary of the Navy Objectives*, and consistent with the overall management guidance in the *President's Management Agenda* and the *21st Century Seapower Strategy.*

The *OPNAV N6/Deputy DON CIO (Navy) Strategy* and the *Marine Corps Integrated Communications Strategy* are similarly aligned to the *DON IM/IT Strategic Plan* and are collectively driving the definition and rollout of key programs such as the Next Generation Enterprise Network, the DON's next generation IM/IT infrastructure. This strategic alignment validates the vision, mission, and goals of the *DON IM/IT Strategic Plan* ensuring common goals, objectives, and performance measures. The DON's ability to continue and build on this alignment is critical to providing the naval warfighter with the tools needed to win.

The graphic below depicts the alignment of these key documents using Goal #2 of the *DON IM/IT Strategic Plan* as an example of



STRATEGIC PLANNING PROCESS

> *"The process we go through to develop the strategic plan is as valuable as the actual document we end up with. Going through this process forces us to take time out from our day-to-day tasks to focus on what we should be doing, rather than what we are doing, and reach consensus on the way ahead."*
>
> Robert J. Carey
> Department of the Navy Chief Information Officer
> September 2007

This is the fifth *DON IM/IT Strategic Plan* published by the DON Chief Information Officer (CIO). We have seen numerous successes during the past two fiscal years, some of which are highlighted in the success stories associated with each goal of this plan.

In this strategic planning cycle, we continue to use the vision, mission, and goals that were developed to span the time frame from FY 2006 through FY 2013. They provide the long-term focus and direction for the DON IM/IT Investment Guidance, which serves as the basis for approving the funding and procurement of all DON IM/IT initiatives.

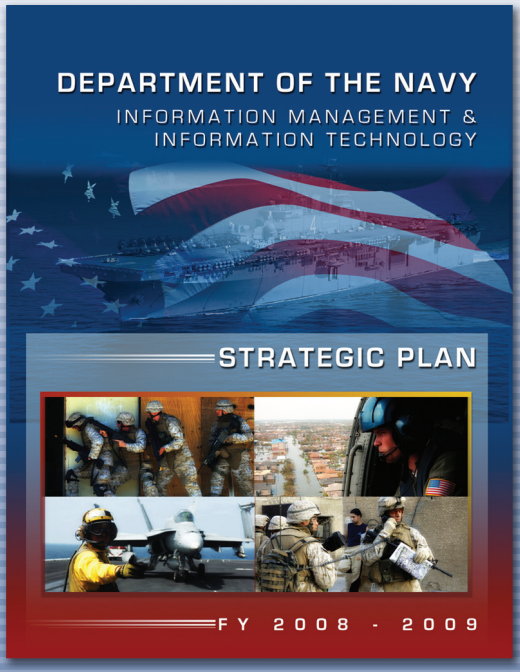
The *DON IM/IT Strategic Plan, FY 2008-2009*, specifies the objectives that will be implemented for each goal during this two-year period. The Department is consistently working to define and refine performance metrics for the objectives in this plan, so that our progress can be clearly measured.

This DON IM/IT strategic planning process provides the methodology to move our IM/IT vision, mission, governing principles, goals, and objectives from concept to reality.

MEASURING FOR SUCCESS - LINKING STRATEGY TO EXECUTION

> *"Effective warfighting capabilities require us to optimize Naval cyber, network and communications investments through centralized coordination of requirements, analysis, assessments, and resource programming. We must achieve better fiscal oversight of our taxpayers dollars and remain true to warfighter requirements to deliver the right capabilities at the right time. To ensure success, we must continually measure and assess our cyber effectiveness while remaining aligned to our maritime strategy."*
>
> Vice Admiral Harry B. Harris, Jr.
> Deputy Chief of Naval Operations for Communication Networks (OPNAV N6) and DON Deputy CIO (Navy)
> September 2008

Performance management is a key part of an integrated strategic planning/performance management cycle. The DON IM/IT Performance Measurement Program is designed to bridge the gap between strategic planning and results and help ensure the DON IM/IT organization has the tools and information required to successfully meet its goals and objectives and ultimately, deliver on its mission – to provide the warfighter with the best IM/IT capabilities possible.



Integrated Strategic Planning/Performance Management Cycle

VISION

A Naval warfighting team armed with the secure, appropriate, assured, accurate, and timely information to fight and win.

MISSION

Deliver secure, interoperable, and integrated IM/IT capabilities to the Marine and Sailor to support the full spectrum of warfighting and warfighting-support missions.

GOVERNING PRINCIPLES

The Navy-Marine Corps IM/IT team will:

- Deploy interoperable, Joint IM/IT solutions to enhance warfighter effectiveness.
- Align Department-wide IM/IT efforts with warfighter priorities.
- Assure global secure access to information.
- Lead continuous capability-enhanced IM/IT transformation.
- Optimize information resources and investments by maximizing return on investments, increasing efficiency, expanding the use of Enterprise solutions, and measuring the contribution of IT investments to warfighting effectiveness.
- Adopt and share best practices.

GOALS

1. Establish and manage a secure, interoperable net-centric Naval IM/IT infrastructure.

2. Protect and defend our Naval critical infrastructures, networks, and information to maximize mission assurance.

3. Accelerate the migration of our applications and data to a net-centric Naval environment to facilitate warfighting and business transformation.

4. Create, align, and share knowledge to enable effective and agile decision making to achieve Knowledge Dominance.

5. Ensure Naval IM/IT investments are selected, resourced, and acquired to deliver affordable enhancements to warfighter effectiveness.

6. Develop an agile and integrated IM/IT total force capable of implementing, operating, and managing the power of the net.

GOAL 1

ESTABLISH AND MANAGE A SECURE, INTEROPERABLE NET-CENTRIC NAVAL IM AND IT INFRASTRUCTURE

> *"Our IT dominance is being challenged—today. While IT can be a strength, it can also be a vulnerability—especially in an economy that is increasingly dependent on IT connectivity. Indeed, high technology communications are ubiquitous and integrated into all aspects of our daily lives. The challenge is for us to ensure that our strength in IT remains an advantage on the battlefield. I hope to impress upon you the urgency of the challenge."*
>
> The Honorable Donald C. Winter
> Secretary of the Navy
> March 2006

DESCRIPTION

We will plan, develop, implement, operate, and sustain a global information infrastructure to provide secure, interoperable, and end-to-end connectivity to all our Sailors, Marines, and Civilians. This infrastructure's common architecture and technical standards will ensure that the Naval component of the DoD Global Information Grid (GIG) maintains interoperability with Joint forces, allied coalitions, and interagency partners.

OBJECTIVES

1.1 Capitalize on investments to the Naval IM/IT infrastructure by transforming the existing enterprise and legacy networks of the DON into a seamless, interoperable, and highly secure net-centric Naval Networking Environment, where data and services are ubiquitously available to all warfighting and warfighting-support users. A critical step in this transformation will be the seamless transition from the existing Navy Marine Corps Intranet (NMCI) to the Department of the Navy's Next Generation Enterprise Network (NGEN).

1.2 Define, implement, and enforce a set of DON IT standards, including a DON-wide strategy for fielding up-to-date operating systems, that enable net-centric operations across the DON enterprise and within Joint and Coalition environments.

1.3 Develop and leverage national and international strategic partnerships to ensure Naval spectrum-dependent systems and equipment have sufficient electromagnetic spectrum available for operations and training.

1.4 Implement an enterprise approach to telecommunications within the Department, ensuring a robust infrastructure with improved financial management and leveraging new technologies to provide maximum capability to our Sailors and Marines for mission accomplishment.

1.5 Develop, implement, and enforce a set of IT standards that support DON operational requirements within a Joint Information Environment.

KEY PERFORMANCE INDICATORS

- Develop the plan to transition from NMCI to NGEN
- Reduce or rationalize the number of networks/points of presence within the DON Naval Networking Environment
- Accelerate network and applications migration to current or immediate predecessor versions of applications and network operating system software

SUCCESS STORIES

COMPUTER NETWORK DEFENSE

Information must be both secure and available to the warfighter. The DON is working to ensure availability of its networks and information, while providing, to the maximum extent possible, information security. The warfighter needs to know that the information he or she is receiving and transmitting is accurate, secure, available, and authenticated to the correct users. Yet, the threats to information security and availability increase daily.

The DON has taken several significant steps to improve its Computer Network Defense, including:

- Submitting and approving information assurance (IA) strategies for major IT systems, in accordance with the Clinger-Cohen Act;
- Achieving greater than 90 percent adherence within NMCI to cryptographic logon (CLO) and public key infrastructure (PKI) requirements, using the common access card (CAC) to access NMCI and associated systems. Next efforts will be devoted to outside the continental United States and afloat CLO/PKI;
- Achieving the President's Management Agenda (PMA) GREEN status (greater than 90 percent adherence) for system security certification and accreditation (C&A) as well as Federal Information Security Management Act (FISMA) required security reviews and testing;
- Achieving PMA GREEN status for submission of privacy impact assessments of DON systems, thereby providing greater privacy protection for departmental personnel and their families;
- Developing policies for data at rest, personal electronic devices, and remote access to DON networks, and updating general DON IA policy to protect the Department's information;
- Coordinating with the Defense Information Systems Agency, National Security Agency, Navy Cyber Defense Operations Command, Marine Corps Network Operations and Security Command, as well as the Naval Criminal Investigative Service, to monitor, investigate, and respond to network intrusions, and develop improvements to security tools and defense mechanisms;
- Overseeing IA practices throughout the Department in coordination with the Naval Audit Service and the Naval Inspector General.

Computer Network Defense is vital. It is the DON's top priority and must be approached aggressively at all levels because the warfighter depends on the validity and availability of the information he or she receives and transmits.

ELECTROMAGNETIC SPECTRUM LEADERSHIP FOR CHANGE

Network-centric warfare is impossible without access to the electromagnetic spectrum. Naval communications, radar, air and fleet defense, weapons guidance, command and control, and many other systems rely on electromagnetic spectrum for their operations. The accelerated development of electromagnetic spectrum-dependent devices around the globe has resulted in a shortage of this finite resource. To meet the growing demand, new electromagnetic spectrum-efficient technologies are emerging. These include Software Defined Radio, Policy Based Radio, Cognitive Radio, and other advanced radio technologies. Internationally recognized as a fair and honest broker, members of the DON Electromagnetic Spectrum Team chair or hold seats in forums within the United Nations International Telecommunications Union which establishes international radio regulations. The Department of the Navy is reshaping the electromagnetic spectrum landscape of today to empower the warfighter of tomorrow.

JOINT INFORMATION ENVIRONMENT – MARIANAS

Guam and the Northern Mariana Islands are becoming the linchpin of the Armed Forces' western Pacific presence. Designated as a Joint Region, the area will host expanded Air Force and Navy operations as well as new Army and Marine Corps detachments. As Executive Agent for the region, the DON is responsible for providing many of the common supporting services including Information Management (IM) and Information Technology (IT) resources.

To meet this responsibility the DON has led a Joint effort to define and deliver the future IM and IT environment, known as the Joint Information Environment – Marianas (JIE-M). Accomplishments to date include an analysis and recommendations on the Joint IT backbone on Guam; engineering sessions to further develop the backbone infrastructure; and strategic planning sessions to begin the analysis and develop options on additional IT resources. Areas studied included wireless networking, satellite communications, and land mobile radios as well as methods of best delivering network operations, identity management, and authentication services in a Joint environment.

It is expected that not only will JIE-M provide an exemplary net-centric environment for warfighters operating in the region, but it will also serve as a model for other Joint environments.

GOAL 2

PROTECT AND DEFEND OUR NAVAL CRITICAL INFRASTRUCTURES, NETWORKS, AND INFORMATION TO MAXIMIZE MISSION ASSURANCE

> *"We are increasingly fighting our adversaries in cyberspace as well as traditional warfare domains. Robust defense-in-depth and defense-in-breadth strategies are essential to protect and defend our information superiority so we can continue to dominate in those traditional battle spaces."*
>
> John J. Lussier
> DON Deputy CIO (Policy and Integration)
> September 2007

DESCRIPTION

We will actively defend our people, information resources, and critical infrastructures to provide assured information delivery, system and network access, and information protection. The security and protection of our systems, networks, and information depend on the implementation of sound information assurance concepts and principles across programs and platforms. To this end, we will establish world-class information assurance and system security protocols on all DON networks. Implementing Critical Infrastructure Protection (CIP) measures will protect, defend, and secure our mission-critical capabilities, and ensure that information is available and secure. While maintaining security is vitally important, information must be available to the warfighter in the field. Anticipating verifiable threats, mitigating identified vulnerabilities, and employing proactive self-defense protection strategies, while ensuring availability, will enable effective net-centric operations.

OBJECTIVES

2.1 Use DoD and Federal capabilities to centrally manage associations of people with network devices.

2.2 Protect information to safeguard data as it is being collected, analyzed, processed, and disseminated, and continually mitigate internal and external vulnerabilities, to ensure all information in our dynamic environment has a level of trust and integrity commensurate with mission objectives in support of decision making.

2.3 Identify existing or potential vulnerabilities to the DON critical, physical, and cyber infrastructure through comprehensive assessments, in order to support informed risk mangement decisions.

2.4 Establish a consistent DON Certification and Accreditation (C&A) process that is aligned with Federal and DoD processes while maintaining Federal Information Security Management Act requirements.

2.5 Protect personally identifiable information (PII) and other sensitive unclassified information on portable computing devices, mobile assets, and mobile storage media by implementing a data at rest encryption solution.

2.6 Provide effective Computer Network Defense tools and infrastructure that monitor and respond to attacks, maintain critical communications abilities, and prevent unauthorized access to ashore, afloat, and deployed systems.

2.7 Ensure information and network availability, reliability, and integrity by leveraging defense-in-depth and defense-in-breadth, actively measuring success by conducting vulnerability assessments and assist visits, exercising contingency and continuity of operations plans, and monitoring intrusion statistics.

KEY PERFORMANCE INDICATORS

- Increase the percentage of DON systems compliant with FISMA standards (e.g., current Authority to Operate (ATO), Security testing, COOP testing)
- Increase the percentage of systems that have completed privacy impact assessments (PIA)
- Provide the CIP Self Assessment Tool to facilitate annual infrastructure vulnerability assessments

SUCCESS STORIES

PROTECTING CRITICAL INFRASTRUCTURES THROUGH VULNERABILITY ASSESSMENTS

A primary component of the DON CIP program is identifying vulnerabilities associated with critical assets that, if exploited, could jeopardize mission execution. These assessments determine whether there are any single points of failure that could result in a potential vulnerability. The DON CIO has teamed with the Naval Criminal Investigative Service (NCIS), which executes the Chief of Naval Operations Integrated Vulnerability Assessment (CNO-IVA) Program. The DON CIO's subject matter experts assess an installation's commercial dependencies and Computer Network Defense capabilities, while the NCIS team assesses the anti-terrorism/force protection posture.

The team uses the *CIP Benchmarks and Standards*, developed by the DoD, to conduct consistent evaluations across installations. Since the inception of this approach in FY 2006, through the end of FY 2007, 10 installations have been assessed.

The team prepares for the assessments by obtaining previous assessment reports and data from the public works officers and commercial utilities that provide service to the installation. During the assessment, the team interviews command personnel and utility employees, and examines pertinent infrastructure.

At the conclusion of the assessment, the installation commander is briefed on potential vulnerabilities, both on and off the installation. As a result, the commander is better able to allocate scarce resources to remedy potential vulnerabilities, which, if not addressed, could affect the installation's ability to complete mission-essential tasks.

PUBLIC KEY INFRASTRUCTURE IMPLEMENTATION (PKI) PLAN

The Marine Corps has been a leader in the DoD implementation and management of Public Key Infrastructure (PKI). Since the activation of DoD PKI in 1999, the Marine Corps has aggressively implemented DoD PKI across the Marine Corps Enterprise Network (MCEN), taking advantage of the security services PKI provides, such as non-repudiation, confidentiality, and integrity.

Since the inception of DoD PKI, the Marine Corps has systematically implemented the infrastructure necessary to successfully meet DoD PKI requirements. This implementation includes the issuance of public key certificates to individuals and servers, as well as development of the infrastructure to validate certificates for individual network usage. Providing certificates to individuals is accomplished primarily through the issuance of the DoD-mandated Common Access Card (CAC). The Marine Corps has successfully issued more than a half million CACs, all of which hold public key certificates for use by individual Marines, government personnel, and authorized contractors.

2007 FISMA STATUS

The Navy and Marine Corps achieved GREEN status (greater than 90 percent compliance) in the President's Management Agenda for Federal Information Systems Management Act (FISMA)-required system certification and accreditation, system security review, security controls tested, and contingency plan testing. This achievement was accomplished through close coordination and monitoring by DON CIO and Navy/Marine Corps headquarters personnel, and more importantly, through detailed attention to the task by Marine Corps Systems Command, Navy Echelon II commands, command information officers, and information assurance managers. Annual security awareness training and IT workforce training requirement rates in both the Navy and Marine Corps exceeded DoD goals for both training and certification for the year.

DIACAP TRANSITION

In November 2007, the Department of Defense issued DoD Instruction 8510.01, DoD Certification and Accreditation Process (DIACAP), replacing its DITSCAP instruction of 1997. Using Lean Six Sigma processes and with close coordination among the DON CIO, Navy, Marine Corps, and the respective operational Designated Accrediting Authorities (DAAs), the DON produced a DIACAP Transition Guide and DIACAP Handbook to aid the transition and provide step-by-step guidance on the new certification and accreditation process. Additionally, the DON conducted extensive research into automated tools for use across the Department to support DIACAP implementation and execution, and is in the process of selecting a tool.

GOAL 3

ACCELERATE THE MIGRATION OF OUR APPLICATIONS AND DATA TO A NET-CENTRIC NAVAL ENVIRONMENT TO FACILITATE WARFIGHTING AND BUSINESS TRANSFORMATION

> *"In order to obtain the best value and flexibility to meet our operational requirements, we must have a balance between accessibility, security, and the fiscal environment. We must look at innovative, cost-effective solutions that can be easily implemented and can quickly increase in capability and capacity."*
>
> Brigadier General George J. Allen
> Director, Command, Control, Communications, and Computers (C4), and DON Deputy CIO (Marine Corps)
> September 2008

DESCRIPTION

We will implement a Navy and Marine Corps Portal strategy that will provide the single sign-on gateway to the Department's core enterprise applications, services, and processes. This strategy will align with DoD and Joint efforts. We will intensify our efforts to eliminate legacy networks, servers, systems, applications, and duplicative data environments. We will transform proprietary and tightly coupled systems and applications into a set of enterprise services that emphasize loosely coupled systems and processes. These enterprise services will be leveraged across the Department to provide seamless connectivity to mission critical information.

OBJECTIVES

3.1 Identify and eliminate stove-piped legacy networks, monolithic systems and applications, and duplicative data sources that hamper our ability to achieve a net-centric mode of operations. Continue initiatives such as the Navy's Cyber Asset Reduction and Security (CARS) program and Marine Corps' Legacy Network Consolidation (LNC) efforts. Accelerate these efforts as necessary to support the implementation of the DON Next Generation Enterprise Network (NGEN).

3.2 Transform proprietary systems and applications into an open architecture-compliant authoritative set of enterprisewide services and processes, in accordance with the concepts of a Service Oriented Architecture.

3.3 Develop and promulgate the DON Net-Centric Data Transformation Plan, which will link Functional Data Managers and DoD Community of Interest processes.

3.4 Identify and designate departmentwide authoritative data sources and authoritative enterprise services.

3.5 Implement a Navy Marine Corps Portal strategy that consolidates and federates existing Navy and Marine Corps portals that align and leverage DoD portal initiatives.

KEY PERFORMANCE INDICATORS

- Number of legacy networks, servers, systems, applications eliminated by CARS and LNC initiatives
- Number of authoritative data sources identified and number of duplicative data sources eliminated across the Department
- Number of portals consolidated and eliminated as a result of the publication of a DON portal alignment strategy

SUCCESS STORIES

CYBER ASSET REDUCTION AND SECURITY

The DON Deputy CIO (Navy) has taken the lead for the Navy's IT investments to improve Navy enterprisewide IT security, interoperability, and return on investment, and prepare for the NGEN environment.

DON Deputy CIO (Navy) initiated and then combined two efforts — Capture the Money (CTM) and Cyber Asset Reduction and Security (CARS) — to assess Navy IT investments, achieve total IT asset cost visibility, and identify IT resource realignment opportunities.

To establish total IT asset cost visibility, a CTM IT Budget Stewardship Review team was formed to provide current year management and oversight, identify where money is being spent, and apply uniform stewardship evaluation criteria. The team will assess the IT budget by command, to track, analyze, and evaluate IT-related financial data, ensure compliance with legal and regulatory documents and plans, and develop IT funding realignment recommendations.

The CARS initiative (formerly Legacy Network Reduction) works to identify policies to support optimum alignment of Navy IM/IT resources in support of a functional net-centric information environment. By CY 2008, CARS will ensure the Navy achieves and maintains ashore IT asset visibility (cost, configuration, and accountability) in preparation for a post-NMCI environment. By September 2010, CARS will ensure the Navy dramatically reduces its ashore IT footprint of networks, systems, servers, and applications while improving enterprise security and optimizing IT investments. This will be accomplished by realigning resources as required, based on the reduction of the Navy's ashore IT footprint.

MARINE CORPS CENTER FOR LESSONS LEARNED MANAGEMENT SYSTEM

The Marine Corps Lessons Learned Program was established to enable the Commandant of the Marine Corps to fulfill Title 10 responsibilities (to organize, train, equip, and provide Marine Forces). It also provides robust support to the Joint Lessons Learned Program by capturing knowledge and experience related to systems, tactics, techniques, and procedures to remedy deficiencies and reinforce successes.

The Marine Corps Center for Lessons Learned (MCCLL) was developed to serve as a single fusion center to collect, analyze, manage, and disseminate knowledge gained through operational experiences, exercises, and supporting activities. MCCLL enables Marines to achieve higher levels of performance and provides information and analysis on emerging issues and trends in support of operational commanders and the Commandant of the Marine Corps. The Lesson Management System (LMS) is designed to manage the Marine Corps lesson collection, tracking, data-mining, and dissemination requirements.

In April 2006, the Director for Operational Plans and Joint Force Development (Joint Staff J-7) selected the MCCLL LMS as the DoD lessons learned input support tool. Since that time, the MCCLL, working with the Joint Staff, evolved the LMS into the Joint Lessons Learned Information System (JLLIS) and worked with U.S. Joint Forces Command and Joint Center for Operational Analysis to develop the Joint Lessons Learned Repository (JLLR). The JLLIS/JLLR provides net-centric data sharing across the Joint lessons learned community of practice and enables one-stop access to federated data (from the Services, combatant commands, and combat support agencies). It also provides an enterprise-level document management capability to extract trends, conduct pattern analysis, and cross-map solutions to identified shortfalls. The MCCLL has standardized and improved information delivery to all authorized DoD users conducting a federated search of Marine Corps lessons learned.

GOAL 4

CREATE, ALIGN, AND SHARE KNOWLEDGE TO ENABLE EFFECTIVE AND AGILE DECISION MAKING AND TO ACHIEVE KNOWLEDGE DOMINANCE

> *"Our Naval networks must adopt compatible core services, implement compatible data strategies, and adopt compatible software to ensure seamless interoperability. This will facilitate knowledge sharing and enable effective command and control. Seamless data sharing aligned with effective cyber networks are critical to achieving decision superiority for the warfighter."*
>
> Vice Admiral Harry B. Harris, Jr.
> Deputy Chief of Naval Operations for Communication Networks (OPNAV N6) and DON Deputy CIO (Navy)
> September 2008

DESCRIPTION

We will integrate technology and processes within FORCEnet to effectively provide secure, assured, accurate, and timely information to the warfighter. We will enable the information value chain of identity management, information assurance, authoritative data bases, fast and accurate search, and content management to effect knowledge management. This rapid exchange of all source knowledge will be critical to the effective employment of our vast intelligence capability, battlefield awareness insight, and weapons capabilities. Similarly, we will emphasize seamless knowledge transfer between people and applications in designing and deploying future support processes. We will move from a culture that rewards the retention of data and information to one that rewards effective knowledge stewardship.

OBJECTIVES

4.1 Establish processes within the Enterprise and create functional communities of practice to enable net-centric knowledge sharing.

4.2 Implement a comprehensive standards-based content management strategy Departmentwide.

4.3 Manage records effectively and continue Departmentwide implementation of Electronic Records Management (ERM).

4.4 Manage bandwidth constraints to support rapid knowledge exchange, particularly for tactical users.

4.5 Define the architecture and way ahead to enable net-centric information sharing to achieve Maritime Domain Awareness, in order to facilitate effective decision making for all maritime related missions.

KEY PERFORMANCE INDICATORS

- Increase the number of enterprise processes using net-centric knowledge sharing
- Measure progress toward implementation of Enterprise ERM
- Develop and promulgate the DON content management strategy

SUCCESS STORIES

INDIVIDUAL AUGMENTEE COMMUNITY OF PRACTICE

During the GWOT, numerous Navy personnel have served in unfamiliar roles. Because few Sailors have working knowledge of combat operations ashore, the Navy has relied on the Army for training. However communicating pertinent information to the Sailors selected for augmentee missions posed a challenge due to the abundance of available information. Navy Knowledge Online (NKO) was chosen to host an online location, or Community of Practice (CoP), for Sailors to do "one-stop shopping" for the information they would need before deploying.

Ensuring the accuracy and accessibility of the posted information is critical to implementing a successful solution. Therefore, to gather information for the CoP, the Navy met with the Army team responsible for outfitting, training, and transferring the augmentees from the continental U.S. to various locations supporting the GWOT.

Accessible and user friendly, the CoP provides pages for each country to which Sailors are deploying, including key points of contact, maps, and other important information. It includes a list of required Navy e-learning courses and a discussion forum for deploying and deployed personnel to share unclassified information pertaining to daily life in the U.S. Central Command area of responsibility. The CoP also has a page on cultural "do's and don'ts," validated by the Knowledge Management teams at the Center for Naval Intelligence and Center for Information Dominance.

After the CoP was developed and made visible to NKO users, it took just one day for the first feedback submission to be posted. From a KM perspective, this CoP has all the ingredients of a successful collaborative tool. The Individual Augmentee CoP provides timely and accurate information that assists individual augmentees in their support of the GWOT.

MARFORRES TRANSITION TO NET-CENTRIC ENTERPRISE SERVICES

Marine Forces Reserve (MARFORRES) lacked a web-based collaboration environment for its multiple distributed subordinate units. During the past year, MARFORRES has expanded its intelligent collaboration portal, enabling out-of-the-box functionality, and efficient and cost-effective expansions and enhancements. In addition, the portal has enabled integration with familiar tools and the ability to deploy organization wide standards, which provide persistent security, management, and integration on a scalable platform. The MARFORRES portal is an enterprise business solution that provides a single sign-on capability, greatly easing user access to enterprise business applications such as Training and Exercise Employment Plan, Memorandum Fiscal Services, Marine Corps Enlisted Administration Separations, and Reserve Order Writing System.

The MARFORRES portal facilitates end-to-end collaboration through the use of aggregation, organization, and search capabilities. Across MARFORRES, there are 4,500 registered users, who have stored more than 32 gigabytes of relevant information within the collaboration site. The portal content and information layout can be customized for specific audiences.

MARFORRES organizations can target information, programs, and updates to audiences based on their organizational role, team membership, interest, security group, or any other criteria important to the commander. The MARFORRES portal enables a net-centric environment that facilitates collaboration and access to enterprise services for authorized users within the Reserve component.

GOAL 5

ENSURE NAVAL IM AND IT INVESTMENTS ARE SELECTED, RESOURCED, AND ACQUIRED TO DELIVER AFFORDABLE ENHANCEMENTS TO WARFIGHTER EFFECTIVENESS

"Transformation is never complete; it is a constant process and attitude. Our new Maritime Strategy and our ongoing transformation efforts, within the framework of Seapower 21, guide the Navy's future direction. I believe we are already making great strides in developing the capabilities we will need in coming years. Areas of particular interest include cyberspace, unmanned systems, and Maritime Domain Awareness."

Admiral Gary Roughead
Chief of Naval Operations
October 2007

DESCRIPTION

We will select efficient and effective IM/IT investments based on validated user requirements. Investments will align with strategic priorities, established in Presidential, Federal, DoD and DON guidance; align with the DoD Global Information Grid (GIG) strategy for implementation of net-centricity and the Business Enterprise Architecture; and be interoperable within the Joint and Coalition environments. Cost visibility and uniform evaluation criteria will provide the ability to quantify the return on investment and total cost of ownership in a standard manner across all programs.

OBJECTIVES

5.1 Implement DON portfolio management policies and procedures that provide a standard process for the selection and management of IT/National Security Systems investments in support of mission area capability requirements.

5.2 Implement a DON Enterprise Architecture (EA) Strategy in support of critical IT investment management decision making that will create an authoritative federated enterprise architecture, resulting in a consistent set of departmental and Service level EA policies and establish an effective overarching EA governance process.

5.3 Develop and manage DON Functional Area Manager (FAM) enterprise transition plans supporting the migration to DON core applications and systems that meet the functional/mission area and enterprise capabilities.

5.4 Implement a DON-wide IT Asset Management (ITAM) process that builds on the FAM governance structure, meets the ITAM requirements of the DoD and President's Management Agenda, and efficiently utilizes the IM/IT Enterprise Agreements to acquire products and services.

5.5 Optimize the telecommunications environment to deliver the right mix of service, asset visibility, and expense management. Institute procedures to ensure graceful degradation of service if necessary to mitigate impacts of a telecommunications infrastructure network attack.

5.6 Leverage DoD and DON enterprise initiatives, such as Defense Knowledge Online (DKO), Net-Centric Enterprise Services (NCES), and Marine Corps Enterprise IT Systems (MCEITS), to the maximum extent practical.

5.7 Engage in DoD's Continuous Process Improvement initiative through Lean Six Sigma activities to support DoD business process improvement efforts.

5.8 Develop and execute outcome-based performance measures to optimize the value of IM/IT investments to the warfighter.

KEY PERFORMANCE INDICATORS

- Increase the percentage of IT systems registered in DITPR-DON whose budgets have been identified in NITE/STAR
- Reduce the number of legacy and interim applications
- Increase the percentage of FAMs with enterprise transition plans
- Publish the DON ITAM Implementation Plan

SUCCESS STORIES

REAL TIME GLOBAL WARFIGHTER SUPPORT

The Naval Air Systems Command provides new and improved weapons systems to the warfighter by supporting technology for the 3,800 manned and unmanned aircraft in the Navy and Marine Corps inventory. Airworthiness and flight safety instructions for these weapons systems are provided in flight clearance documents. The paper-based process to generate a flight clearance could take as long as 45 days, which often resulted in forces engaging threats with older technologies while waiting for new capabilities to be certified.

To reduce the turnaround time, a paperless, fully automated process that allows parallel reviews was introduced. This capability permits the engineers to securely review flight clearances from anywhere in the world, eliminating delays based on geographical location. In less than three months, turnaround time for the review of flight clearances was reduced to less than two days for deployed forces. In some cases, deployed forces have received new capabilities in response to a changing threat in less than two hours.

This enhanced IT capability, which will increase as the process becomes web-centric, has saved the DON millions of dollars through enhanced efficiency. More importantly, it is saving the lives of front-line forces because they have the most effective weapons systems available to them faster.

USMC CONDOR CAPABILITY SET

Operation Iraqi Freedom highlighted the need for improved on-the-move and beyond-line-of-sight data capabilities for maneuver units. Command and Control (C2) On-the-Move Network Digital Over-the-Horizon Relay (CONDOR) provides these capabilities throughout the Marine Air Ground Task Force (MAGTF). CONDOR enables the use of C2 applications and tactical data radios to feed the Common Operational Picture (COP), while on-the-move and over-the-horizon. Building the COP increases situational awareness of friendly units and disseminates intelligence products on enemy locations, significantly enhancing the information available for the leader's decision cycle.

The CONDOR capability set bridges the gap between today's radio inventory and the future Transformational Communication Architecture. CONDOR's fundamental premise is to make the tactical network accessible to the warfighter, using organic Marine Corps assets. This architectural approach is based on open standards that provide encrypted connectivity to the forward edge of the battlefield and will readily accept Joint Tactical Radio System terminals as they are fielded. The CONDOR capability sets are meeting the needs of the operational forces to have C2 on-the-move while conducting operations in Iraq.

GOAL 6

DEVELOP AN AGILE AND INTEGRATED IM AND IT TOTAL FORCE CAPABLE OF IMPLEMENTING, OPERATING, AND MANAGING THE POWER OF THE NET

> *"The development and retention of quality people are vital to our continued success. America's Naval forces are combat-ready due to the dedication and motivation of individual Sailors, Marines, Civilians, and their families. The Department is committed to taking care of them by sustaining our quality of service/quality of life programs, including training, compensation, and promotion opportunities, health care, housing, and reasonable operational and personnel tempo. The cost of manpower is the single greatest factor in the FY 2008 budget, but it is money well spent. We must continue to recruit, retain, and provide for our Sailors and Marines."*
>
> The Honorable Donald C. Winter
> Secretary of the Navy
> March 2007

DESCRIPTION

We will execute DON IM/IT total workforce objectives in a manner that ensures the workforce is postured to execute current and emerging missions, while ensuring effective and efficient use of emerging technologies and concepts. We recognize that the execution of DON missions is driven by the collective talent, skills, and capabilities of our IM/IT professionals. A major challenge we face in the future is staying attuned to the needs and capabilities of our multi-generational workforce, including our Millennial Generation Sailors and Marines who have a greater expectation of the incorporation of technological capabilities into their everyday lives. As the DON and DoD move from organizational to net-centric operations, and implement the policies and technologies necessary to support that transformation, we will ensure that the critical success factors necessary to identify, develop, and support the DON IM/IT workforce are accounted for in workforce strategy planning and execution.

OBJECTIVES

6.1 Identify the IM/IT workforce manpower, personnel, and training requirements for next generation DON information technology.

6.2 Reassess, validate, and transition to a net-centric IM/IT workforce through fundamental changes in policy, processes, and culture.

6.3 Align IM/IT workforce roles, responsibilities, and capabilities through the identification and development of common competencies, to include the program and project management skill sets necessary to successfully develop, operate, and maintain today's complex systems.

6.4 Strengthen the identification, training, certification, and management of an IA workforce that is capable of protecting information, defending systems and networks, providing integrated IA situational awareness, and transforming and enabling IA capabilities.

6.5 Attract, develop, and retain a highly capable IM/IT workforce with the mission critical competencies and capabilities required to support DON missions.

KEY PERFORMANCE INDICATORS

- Increase the percentage of IA workforce positions filled with certified personnel
- Increase the percentage of the workforce that has completed annual IA awareness training
- Increase the percentage of infusion of new talent

SUCCESS STORIES

LEADING THE WAY IN IA WORKFORCE MANAGEMENT

DON commands are making significant progress to meet the Information Assurance (IA) Workforce Transformation commercial certification requirements. Some examples and best practices include:

- Navy Network Warfare Command and Marine Corps Headquarters IA workforce managers are funding commercial certification classes in large numbers and sharing course seats to gain economies of scale.
- Naval Supply Systems Command hosted a course for 127 IA managers.
- Naval Safety Command has already met its goal of 100 percent certification of its IA workforce.
- Navy Military Medicine implemented training using the virtual environment and pre-assessments to identify curricula to close its IA knowledge gaps.
- U.S. Marine Corps Forces Command improved reporting relationships and process flow by increasing its IA workforce.
- Naval Education and Training Command realigned its IA workforce to streamline and improve communications.
- Navy Personnel Command clarified operational and administrative chain-of-command responsibilities for the IA workforce.
- Space and Naval Warfare Systems Command, with more than 2,500 IA positions, has embarked on a comprehensive plan to ensure targeted training and certification.
- Commander U.S. Pacific Fleet and Commander U.S. Fleet Forces Command are working, with the other Type Commanders, to commercially certify all IA personnel aboard ships, implement a metrics program aligned to the Defense Readiness Reporting System, build the Navy IA Mission Essentials Task Lists, and integrate an inspector general program to ensure FISMA compliance.

Progress like this will continue as the Department makes a major shift in how the IA workforce is certified and managed.

CISCO ACADEMY

The Marine Corps Communication and Electronics School recently established a Cisco Academy where certified Marines teach the Cisco Certified Network Administrator (CCNA) course to military and civilian IT professionals. This on-site training benefits Data Supervisors, Data Chief Marines, and their Commanding Officers by reducing the transit time normally associated with attending these courses. CCNA and the Cisco Certified Network Professional (CCNP) courses, planned for FY08, promise to be beneficial to the Operating Force as IT professionals are certified and training transit time is minimized.

NAVY COOL

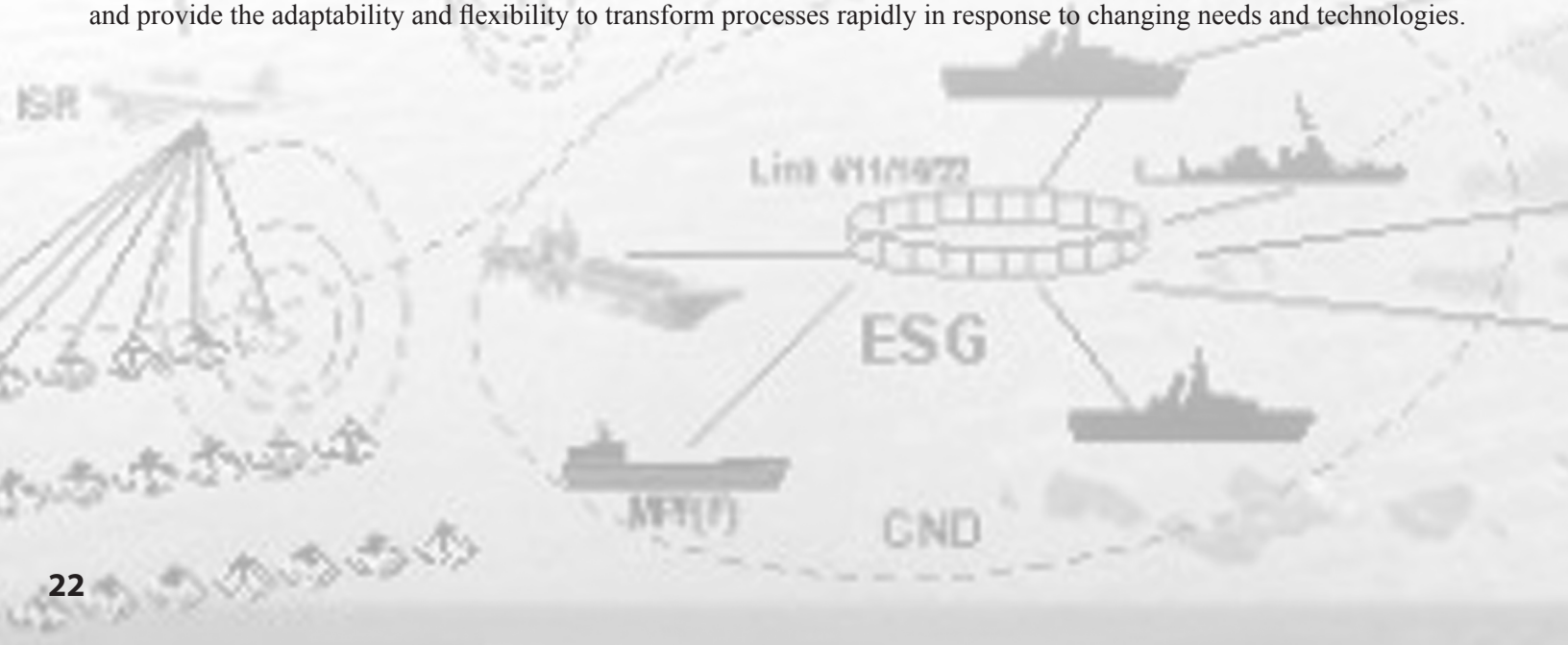
The Navy Credentials Program Office organizes commercial certification processes and buys commercial certification test vouchers at the enterprise level, thereby reducing the cost to individual commands. IA credentialing information and test voucher request forms are accessible via the new "Navy Credentialing Opportunities On-Line" (COOL) web tool. The test voucher request forms allow Sailors to request free commercial certification testing through the Echelon II IA Manager. As DON IA professionals obtain standard credentials, they will be more valuable to operational leaders because they will be interchangeable in performing the Joint IA mission.

FORCENET: AN INTEGRAL PART OF INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY

FORCEnet is the DON's initiative to achieve Net-Centric Operations/Warfare (NCOW) and Joint transformation by providing robust information sharing and collaboration capabilities across the Naval/Joint force. It is the operational construct and architectural framework that accelerates implementation of full IM/IT capability by integrating weapons, sensors, command and control, platforms, and warriors into a secure, networked, distributed force as part of the GIG. FORCEnet is substantially transforming the DON in both process and product:

- The FORCEnet Functional Concept established a Joint, operational foundation for all FORCEnet requirements.
- The FORCEnet Requirements/Capabilities and Compliance (FRCC) Policy codified and implemented FORCEnet requirements, including supporting architectures and standards. These requirements were developed in collaboration with the other Services, the Office of the Secretary of Defense, the Joint Staff, national agencies, combatant commanders, Allied and Coalition partners, and industry to enhance efficiency and interoperability while supporting the Department's integration into the GIG. In FY 2007, this policy was broadened and was integrated into Secretary of the Navy Instruction 5000.2D (Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System), which is projected to be promulgated in FY 2008.
- The FORCEnet Integrated Architecture governance structure provides authoritative Naval Enterprise Architecture products, places these products into configuration management, and disseminates these authoritative architectures into the broader DoD architecture community through the DoD Architecture Registry System (DARS).
- The FORCEnet IT standards governance structure establishes DON enterprise-wide IT standards, places them under configuration management, and disseminates these authoritative IT standards into the broader DoD community through the DoD IT Standards Registry (DISR).
- The Navy Enterprise Architecture and Data Strategy (NEADS) Policy, promulgated by the DON Deputy CIO (Navy) in FY 2007, promotes the alignment of Navy programs and initiatives to DON/DoD guidance.

FORCEnet's integration of tactical and non-tactical systems into a seamless interoperable environment will greatly enhance the sharing of time-critical information. It will ensure the responsiveness of business practices to warfighting requirements and provide the adaptability and flexibility to transform processes rapidly in response to changing needs and technologies.



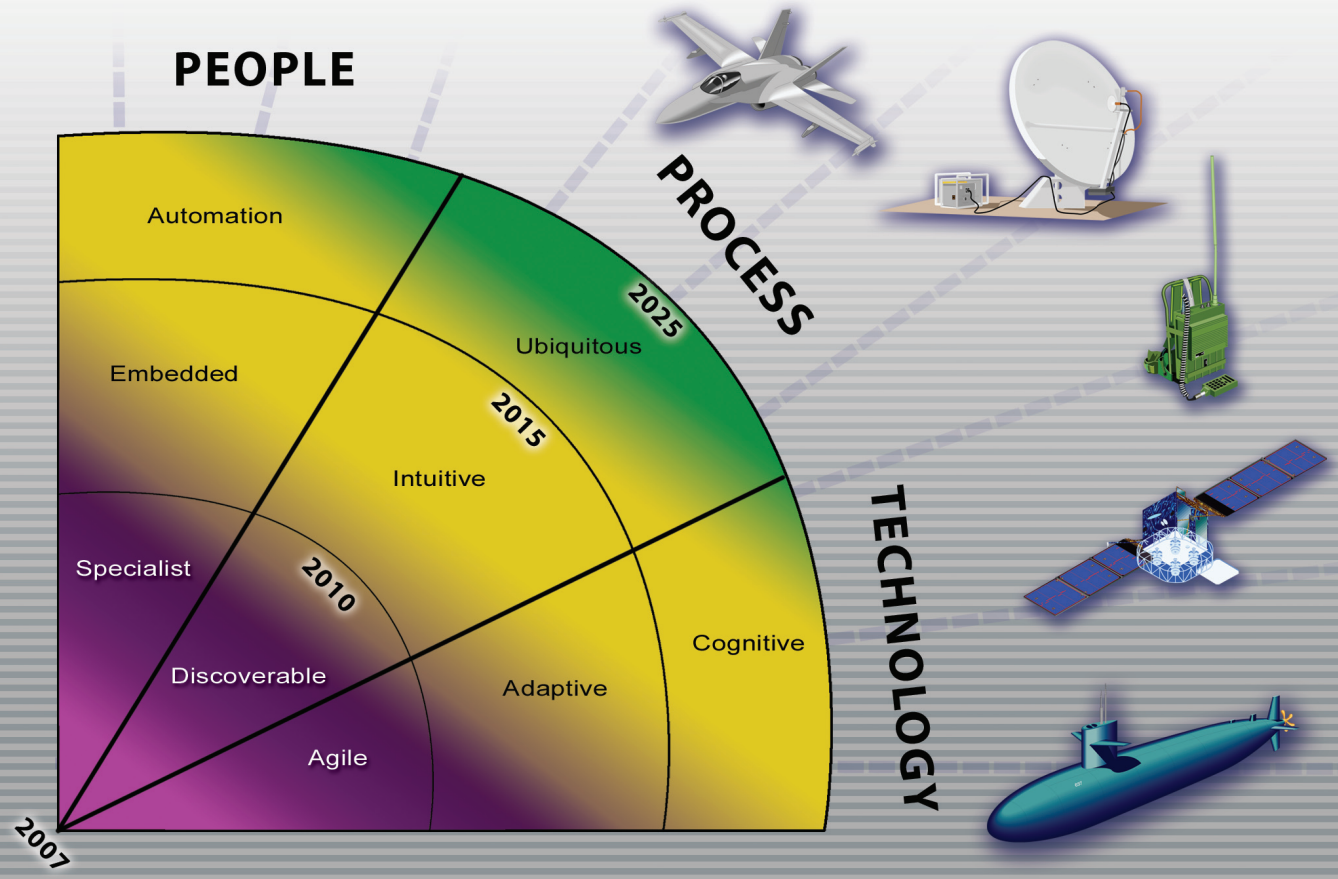
NET-CENTRIC SPECTRUM TRANSFORMATION

As the commercial demand for spectrum increases at a feverish pace, the complexity of enabling global access to the electromagnetic spectrum for the Navy and Marine Corps is growing. Likewise, the Navy and Marine Corps' demand for spectrum is growing as interoperability requirements include spectrum requirements that provide for information sharing and collaboration capabilities across the entire Naval enterprise and the DoD GIG. In this regard net-centric spectrum transformation must be enacted to ensure critical communications, sensors, intelligence, and other spectrum-dependent systems and equipment are fully capable and continue to evolve to better support the Naval warfighter. The spectrum transformation must provide for dynamic and efficient use of the spectrum, and be able to quickly adjust and respond to advanced technologies.

A seamless Net-Centric Spectrum Transformation Plan must be supported by a motivated, capable workforce that includes highly trained and capable spectrum personnel, electronic warfare personnel, and other occupational fields that have vested interests in the use of spectrum. New technologies are continuously being introduced, so the workforce must be skilled in its use of tools that automate many of the spectrum tasks that are now laborious and time consuming. The ability, agility, and adaptability of the spectrum workforce are principal requirements to achieving, implementing, and managing net-centricity.

A tenet in the *DON Strategic Vision for Spectrum* is the continued development of dynamic automation that is intuitive and accessible to all Navy and Marine Corps stakeholders, and enables efficient use of spectrum resources. This technology must include legacy capabilities that now exist within the Naval services as well as provide for the control and coordination of new and emerging technologies and the deconfliction of electronic warfare effects.

SPECTRUM MANAGEMENT PROCESS IMPROVEMENT



INFORMATION AND KNOWLEDGE MANAGEMENT

The DON possesses vast quantities of data and information. For many DON systems and processes this is sufficient. Often, however, we need to convert data and information into knowledge. Knowledge is distilled information that is relevant to a decision, process step, or an action. Whereas Information Management focuses on the connectivity and flow of information, Knowledge Management (KM) focuses on operationally relevant information moving, whether pushed or pulled, to those who need it.

- KM is the cornerstone of decision superiority, knowledge dominance, and information superiority.
- KM is the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase command performance.
- KM offers a wide range of principles and tools; implementation is appropriate for all levels of processes.
- KM can improve large enterprise processes and provide knowledge to decision makers. KM can also improve the day-to-day operations of each level of Navy and Marine Corps command.

SEA OF INFORMATION

THE DON CIO LEADERSHIP TEAM

DON CHIEF INFORMATION OFFICER
Robert J. Carey .....*(703) 602-1800*

DON DEPUTY CIO
John J. Lussier.....*(703) 604-7050*

DON DEPUTY CIO (NAVY)
VADM Harry B. Harris.....*(703) 693-7660*

DON DEPUTY CIO (MARINE CORPS)
BGen George J. Allen.....*(703) 693-3462*

Audit Liaison.....*(703) 601-0047*

Clinger-Cohen Act Confirmation and Certification.....*(703) 602-6845*

Command Operations.....*(703) 601-0116*

Computing and Communications Infrastructure.....*(703) 602-6847*

Contracts and Finance.....*(703) 602-6765*

Data Strategy.....*(703) 607-5651*

Enterprise Architecture.....*(703) 602-6847*

Enterprise Licensing and Enterprise Software Initiative.....*(703) 607-5658*

Enterprises Services Management.....*(703) 607-5608*

IM/IT Workforce Management.....*(703) 601-0605*

Information Assurance and Critical Infrastructure Protection.....*(703) 602-6882*

Investment Management.....*(703) 601-0116*

KM/RM and Information Sharing.....*(703) 607-5653*

Legal Counsel.....*(703) 602-2105*

Maritime Domain Awareness .....*(703) 602-5608*

NGEN Business and Acquisition Strategies.....*(703) 601- 3594*

Performance Measurement.....*(703) 602-6812*

Privacy.....*(703) 602-4412*

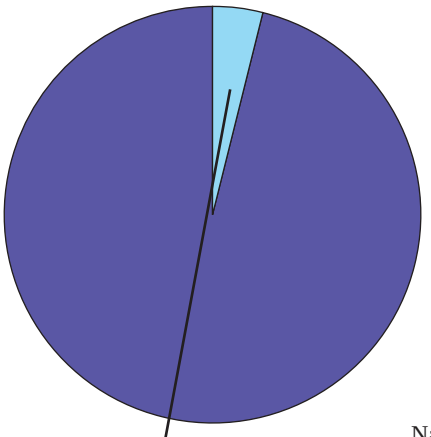
Service Liaison: Navy .....*(703) 602-6800*

Marine Corps.....*(703) 602-6545*

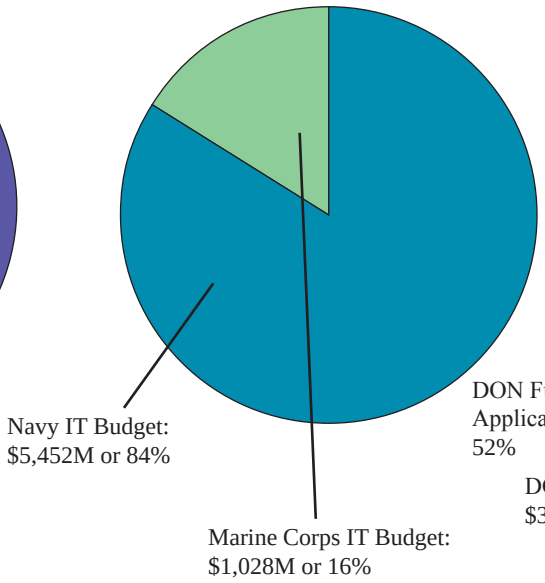
Strategic Planning.....*(703) 602-6812*

DON IT FY 2008 PRESIDENT'S BUDGET REQUEST

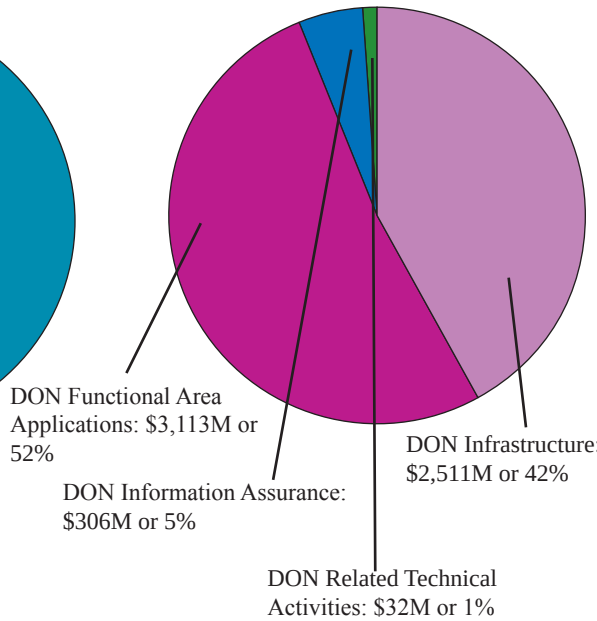
DON Total Obligation Authority Budget Request: $160B



Navy and Marine Corps IT Budget



Navy and Marine Corps IT Budget Breakout



**Totals include Title IX, FY 2007 Supplemental, and FY 2008 GWOT Requests*

ACKNOWLEDGEMENTS

Photographs in this document were supplied by:

- Defense Link Images
- Navy NewsStand
- The Marine Corps Photo Gallery
- DON IM/IT Strategic Plan Working Group

Special thanks to:

- DON IM/IT Strategic Plan Working Group

NOTES

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

TO VIEW ONLINE, DOWNLOAD,
OR REQUEST A COPY OF THIS PLAN:

WWW.DONCIO.NAVY.MIL

Mid-Cycle Updates September 2008

OCTOBER 2007